How to Avoid Falling for Falsehoods:

Mis-, Dis-, and Malinformation (MDM) s

Making good decisions requires having accurate, factual information. At no other point in history have people had as much access to sources of "information". Unfortunately, not all those sources are good. Sources can provide information can be truthful, un-truthful, or an opinion of the writer. Un-truthful information can be spread purposely or accidentally. Un-truthful information that is spread purposely can be done as a satire, to instigate an emotional response or to undermine efforts at making good decisions.

There are now three recognized categories for the outright lies and stretched truths you'll encounter surfing the web: misinformation, disinformation, and malinformation (MDM). Knowing these categories and knowing strategies at identifying good information from bad are important to help you avoid falling for falsehoods.

What is Misinformation, Disinformation, and Malinformation (MDM)?

"Dewey Defeats Truman" happened 75 years ago, but we're all probably aware that misinformation has been increasing since most of us stay connected to the internet for many of our waking hours. You've heard of catfish on dating apps, but some bad actors catfish as online journalists and truth-tellers!

Oftentimes, those spreading disinformation aren't just pranksters – they are trying to influence the public using nefarious means. The people obfuscating the truth online can range from a random Twitter grifter to a whole nation! This topic is heavily politicized now, but it is important to remember that there are countries that try to use disinformation to disrupt the stability of our society.

Media literacy experts have identified multiple strains of untruths that proliferate on the internet.
These different species of "fake news" accelerated in their evolution during the chaos of the COVID-19 pandemic. These species include misinformation, disinformation, and malinformation.

What is Misinformation?

Misinformation refers to false or inaccurate information that a person, account, or group shares without the intention of deceiving others. We might call it rumor, gossip, or tall tales in pre-internet days. Misinformation can spread widely through social media and real-life interactions, and it can even make its way into respected news outlets.

Misinformation usually pops up because of human error, misunderstandings, or fact-checking failures. Some misinformation can be harmless (like your friend misremembering what the weather was like yesterday), but misinformation can also include health-related advice and political falsehoods. Misinformation, then, can have negative impacts because people might make decisions based on untruths.

What is Disinformation?

Disinformation is what most people are referring to when they say “fake news” – information that is patently untrue or misleading and is spread with the intention of misleading other people. Unlike misinformation, which may be unintentional, disinformation is crafted and disseminated with the specific intent to mislead or manipulate.

Disinformation thrives on the savannah of social media, but there are also whole websites that look like legitimate news outlets but trumpet unsourced, made-up news stories. Disinformation is an expanding problem as artificial intelligence programs become widely available because even audio, photograph, and video (maybe you’ve heard of so-called “deep fakes”) can be spoofed.

Usually, the goal of disinformation is to sway public opinion, undermine trust in institutions, or push for specific political, social, or economic outcomes. Countries will hire disinformation-makers to spread fake news along with other cybercrimes.

One real-life example of disinformation involves a coordinated group of social media users tweeting out fake advisories encouraging people to vote in a presidential election via text message, which is not how the election system works. While most people might see this as obviously false, a federal jury thought the people behind the scheme had the intent to deprive others of their constitutional right to vote.

What is Malinformation?

Malinformation, sometimes called “mal-information,” is a newer descriptor of a type of deceptive information you will find online: true information that is deliberately disseminated with the intention to cause harm or inflict negative consequences. Important context, for example, might be removed.

Malinformation involves the selective release or manipulation of truthful information to manipulate public opinion, damage reputations, or provoke unrest. This might include the strategic release of private or sensitive information, the distortion of facts, or the contextual framing of information to deceive or harm individuals or organizations. Malinformation can be employed as a tactic in various contexts, such as political campaigns, online harassment, or even personal vendettas.

How to Avoid Falling for Falsehoods

Combatting misinformation, disinformation, and malinformation in the social media age has proven to be a difficult task for governments, online platforms, news organizations, and the rest of us. Each of us could stand to improve our media literacy, and becoming a sleuth for truth is a habit to be cultivated, not something that can be taught in a few bullet points. You can and should fact-check your government, politicians, and even trusted media outlets – that is your right when you live in a democratic society.

However, there is no reason to despair that the ultimate truth can never be known. Here are some tips for improving your ability to sniff out fake news:

- **Check the source:** Is a bellowing social media account or sketchy “news” website revealing something shocking? Check their sources. Is the “story” based on rumors or random social media chatter? Cross-referencing is excellent for news consumers: use a search engine to see what other news outlets say about the story.
- **Determine the “5 W’s and the H”:** The “5 W’s and the H” is an old journalism trick that can have new life in filtering out fake news. The maxim stands for who, what, when, where, why, and how. Any reporting should answer all these questions. If you read some information, try to answer these questions. Can you pinpoint all 5 W’s and an H in the reporting? Do any seem thin or outright fake?
- **Watch out for manipulation**: Is the information trying to get you to act fast or crafted to make you feel outraged? Peddlers of fake news will try to inspire a sense of urgency, much like the hackers behind phishing attacks. Sometimes they are one and the same.
- **Know your biases:** Every one of us is biased. There are things we are more likely to think are true because of how we see the world. It helps to recognize your biases and consider how they may influence your judgment. Seek our balanced perspectives and diverse sources of information.

- **Have a healthy suspicion of social media:** When it comes to lousy information, social media is like the new playground for all ages. Back in second grade, some kid might have lied about fighting off a tiger. Today, they might post they have the secret for guaranteed weight loss. Before accepting anything you see on social media as accurate, scrutinize it by verifying it independently.

Additional Resources

Evaluating Information: SIFT (The Four Moves)
Disarming Disinformation: Our Shared Responsibility
A Collection of Tips for Combating Online Misinformation Like a Pro
Five new ways to verify info with Google Search
5 tips for not getting tricked online this April Fools' Day — and beyond

---

The information provided in the MS-ISAC Monthly Cybersecurity Tips Newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Disclaimer: These links are provided because they have information that may be useful. The Center for Internet Security (CIS) does not warrant the accuracy of any information contained in the links and neither endorses nor intends to promote the advertising of the resources listed herein. The opinions and statements contained in such resources are those of the author(s) and do not necessarily represent the opinions of CIS.